2/13/2006

In the Claims

Please cancel claims 1—82.

1 ~~83.~~ (New) A method, at least partially implemented by a computer, comprising:

building a data block comprising a first random value and a cryptographic hash of the first random value;

generating, on a second computing device, a signature by digitally signing a string containing a second random value; and

computing an encryption key, for encrypting the data block, by hashing a combination of the signature and a third random value.

2 ~~84.~~ (New) The method as recited in Claim 1 ~~83~~, wherein the second computing device is a smart card.

3 ~~85.~~ (New) The method as recited in Claim 1 ~~83~~, wherein the combination of the digitally signed string and the third random value comprises the digitally signed string concatenated to the third random value.

4 ~~86.~~ (New) The method as recited in Claim 1 ~~83~~, wherein the combination of the digitally signed string and the third random value comprises the third random value concatenated to the digitally signed string.

5 ~~87.~~ 1 (New) The method as recited in Claim ~~83~~, further comprising:

encrypting the data block using the encryption key; and

storing the encrypted data block and the second and third random values.

6 ~~88.~~ 5 (New) The method as recited in Claim ~~87~~, further comprising:

accessing the stored encrypted data block and the second and third random values;

providing a string containing the second random value to the second computing device; and

generating, on the second computing device, a second signature by digitally signing the string containing the second random value.

7 ~~89.~~ 6 (New) The method as recited in Claim ~~88~~, further comprising:

computing a decryption key using the second signature and the third random value;

decrypting the encrypted data block with the decryption key; and

comparing the decryption of the encrypted data block to the data block.

8 ~~90.~~ 7 (New) The method as recited in Claim ~~89~~, wherein computing the decryption key comprises:

hashing the second signature concatenated to the third random value.

9 ~~91.~~ (New) The method as recited in Claim ~~89~~ 7, further comprising:

hashing the first random value contained within the decryption of the encrypted data block; and

comparing the result of this hash with the hash of the first random value contained within the decryption of the encrypted data block.

10 ~~92.~~ (New) A method, at least partially implemented by a computer, comprising:

accessing an encrypted data block, wherein the encrypted data block comprises an encryption of a combination of a first random value and a hash of the first random value;

accessing second and third random values;

providing a string containing the second random value to a second computing device;

generating, on the second computing device, a signature by digitally signing the string containing the second random value; and

computing a decryption key, configured to decrypt the encrypted data block, wherein computing the decryption key uses the signature generated on the second computing device and the third random value.

11 ~~93.~~ (New) The method as recited in Claim ~~92~~ 10, wherein the second computing device is a smart card.

12 10
~~94.~~ (New) The method as recited in Claim ~~92~~, wherein computing the decryption key comprises:

hashing the signature concatenated to the third random value.

13 10
~~95.~~ (New) The method as recited in Claim ~~92~~, further comprising:

decrypting the encrypted data block with the decryption key, wherein the first random value and the hash of the first random value are recovered by the decryption; and

comparing the first random value and the hash of the first random value recovered from the decryption to a data block from which the encrypted data block was generated.

14 13
~~96.~~ (New) The method as recited in Claim ~~95~~, further comprising:

hashing the first random value recovered from the decryption of the encrypted data block; and

comparing the result of this hash with the hash of the first random value recovered from the decryption of the encrypted data block.

15
~~97.~~ (New) One or more computer-readable media comprising computer-executable instructions for encryption-based authentication, the computer-executable instructions comprising instructions for:

building a data block comprising a first random value and a cryptographic hash of the first random value;

generating, on a second computing device, a signature by digitally signing a string containing a second random value; and

computing an encryption key, for encrypting the data block, by hashing a combination of the signature and a third random value.

16
~~98.~~ (New) The one or more computer-readable media as recited in Claim 15
~~97,~~ wherein the second computing device is a smart card.

17
~~99.~~ (New) The one or more computer-readable media as recited in Claim 15
~~97,~~ wherein the combination of the digitally signed string and the third random value comprises the digitally signed string concatenated to the third random value.

18
~~100.~~ (New) The one or more computer-readable media as recited in Claim 15
~~97,~~ wherein the combination of the digitally signed string and the third random value comprises the third random value concatenated to the digitally signed string.

19

~~101.~~ (New) The one or more computer-readable media as recited in Claim 97, further comprising instructions for:

encrypting the data block using the encryption key; and

storing the encrypted data block and the second and third random values.

20

~~102.~~ (New) The one or more computer-readable media as recited in Claim 19 ~~101~~, further comprising instructions for:

accessing the stored encrypted data block and the second and third random values;

providing a string containing the second random value to the second computing device; and

generating, on the second computing device, a second signature by digitally signing the string containing the second random value.

21

~~103.~~ (New) The one or more computer-readable media as recited in Claim 20 ~~102~~, further comprising instructions for:

computing a decryption key using the second signature and the third random value;

decrypting the encrypted data block with the decryption key; and

comparing the decryption of the encrypted data block to the data block.

22
~~104~~. (New) The one or more computer-readable media as recited in Claim 21 ~~103~~, wherein computing the decryption key comprises instructions for:

hashing the second signature concatenated to the third random value.

23
~~105~~. (New) The one or more computer-readable media as recited in Claim 21 ~~103~~, further comprising instructions for:

hashing the first random value contained within the decryption of the encrypted data block; and

comparing the result of this hash with the hash of the first random value contained within the decryption of the encrypted data block.

24
~~106.~~ (New) One or more computer-readable media comprising computer-executable instructions for encryption-based authentication, the computer-executable instructions comprising instructions for:

accessing an encrypted data block, wherein the encrypted data block comprises an encryption of a combination of a first random value and a hash of the first random value;

accessing second and third random values;

providing a string containing the second random value to a second computing device;

generating, on the second computing device, a signature by digitally signing the string containing the second random value; and

computing a decryption key, configured to decrypt the encrypted data block, wherein computing the decryption key uses the signature generated on the second computing device and the third random value.

25
~~107.~~ (New) The one or more computer-readable media as recited in Claim 24 ~~106~~, wherein the second computing device is a smart card.

26
~~108.~~ (New) The one or more computer-readable media as recited in Claim 24 ~~106~~, wherein computing the decryption key comprises instructions for:

hashing the signature concatenated to the third random value.

27
~~109~~. (New) The one or more computer-readable media as recited in Claim 24 ~~106~~, further comprising instructions for:

decrypting the encrypted data block with the decryption key, wherein the first random value and the hash of the first random value are recovered by the decryption; and

comparing the first random value and the hash of the first random value recovered from the decryption to a data block from which the encrypted data block was generated.

28
~~110~~. (New) The one or more computer-readable media as recited in Claim 27 ~~109~~, further comprising instructions for:

hashing the first random value recovered from the decryption of the encrypted data block; and

comparing the result of this hash with the hash of the first random value recovered from the decryption of the encrypted data block.

29
~~111~~. (New) A system configured for encryption-based authentication, comprising:

means for building a data block comprising a first random value and a cryptographic hash of the first random value;

means for generating, on a second computing device, a signature by digitally signing a string containing a second random value; and

means for computing an encryption key, for encrypting the data block, by hashing a combination of the signature and a third random value.

30 ~~112.~~ (New) The system as recited in Claim 29 ~~111~~, wherein the second computing device is a smart card.

31 ~~113.~~ (New) The system as recited in Claim 29 ~~111~~, wherein the combination of the digitally signed string and the third random value comprises the digitally signed string concatenated to the third random value.

32 ~~114.~~ (New) The system as recited in Claim 29 ~~111~~, wherein the combination of the digitally signed string and the third random value comprises the third random value concatenated to the digitally signed string.

33 ~~115.~~ (New) The one or more computer-readable media as recited in Claim 29 ~~111~~, further comprising:

means for encrypting the data block using the encryption key; and

means for storing the encrypted data block and the second and third random values.

34 33

~~116.~~ (New) The system as recited in Claim ~~115,~~ further comprising:

means for accessing the stored encrypted data block and the second and third random values;

means for providing a string containing the second random value to the second computing device; and

means for generating, on the second computing device, a second signature by digitally signing the string containing the second random value.

35 34

~~117.~~ (New) The system as recited in Claim ~~116,~~ further comprising:

means for computing a decryption key using the second signature and the third random value;

means for decrypting the encrypted data block with the decryption key; and

means for comparing the decryption of the encrypted data block to the data block.

36 35

~~118.~~ (New) The system as recited in Claim ~~117,~~ wherein computing the decryption key comprises:

means for hashing the second signature concatenated to the third random value.

37 35

~~119.~~ (New) The system as recited in Claim ~~117~~, further comprising:

means for hashing the first random value contained within the decryption of the encrypted data block; and

means for comparing the result of this hash with the hash of the first random value contained within the decryption of the encrypted data block.

38

~~120.~~ (New) A system configured for encryption-based authentication, comprising:

means for accessing an encrypted data block, wherein the encrypted data block comprises an encryption of a combination of a first random value and a hash of the first random value;

means for accessing second and third random values;

means for providing a string containing the second random value to a second computing device;

means for generating, on the second computing device, a signature by digitally signing the string containing the second random value; and

means for computing a decryption key, configured to decrypt the encrypted data block, wherein computing the decryption key uses the signature generated on the second computing device and the third random value.

39 38

~~121.~~ (New) The system media as recited in Claim ~~120~~, wherein the second computing device is a smart card.

40 38

~~122.~~ (New) The system as recited in Claim ~~120~~, wherein computing the decryption key comprises:

means for hashing the signature concatenated to the third random value.

41 38

~~123.~~ (New) The system as recited in Claim ~~120~~, further comprising:

means for decrypting the encrypted data block with the decryption key, wherein the first random value and the hash of the first random value are recovered by the decryption; and

means for comparing the first random value and the hash of the first random value recovered from the decryption to a data block from which the encrypted data block was generated.

42 41

~~124.~~ (New) The system as recited in Claim ~~123~~, further comprising:

means for hashing the first random value recovered from the decryption of the encrypted data block; and

means for comparing the result of this hash with the hash of the first random value recovered from the decryption of the encrypted data block.